

12:16 pm, Mar 08 2021

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DeputyIN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLANDIN THE MATTER OF THE SEARCH OF
TWO ELECTRONIC DEVICES
CURRENTLY IN THE CUSTODY OF
ATF AT THE BALTIMORE
HEADQUARTERS

Case No. 1:21-mj-461 TMD

**AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT**

I, Joshua Futter, Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), being first duly sworn, hereby depose and state as follows:

I. PURPOSE OF THIS AFFIDAVIT

1. I submit this affidavit in support of a search warrant authorizing the search of a:

a. Black Apple iPhone, model 8 Plus, bearing IMEI No. 352978098922611
(SUBJECT TELEPHONE 1); and,

b. Black and silver Apple iPhone, model 6s, bearing IMEI No. 353338075591211 **(SUBJECT TELEPHONE 2), (collectively, the SUBJECT TELEPHONES).**

2. The **SUBJECT TELEPHONES** are further described in Attachment A and are presently in the custody of the ATF Baltimore Group II Field Office at 1800 Washington Boulevard, Baltimore, in the District of Maryland.

3. I submit that there is probable cause to believe that the **SUBJECT TELEPHONES** contain evidence of Possession of a Firearm by a Prohibited Person in violation of 18 U.S.C. § 922(g)(1) (the **SUBJECT OFFENSE**).

II. AFFIANT BACKGROUND AND EXPERTISE

4. I am “an investigative or law enforcement officer” of the United States within the

meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

5. I have been employed by the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) as a Special Agent since April of 2020. I am assigned to the Baltimore Field Division, Baltimore Group II. I have received training through the Federal Law Enforcement Training Center, located in Glynco, Georgia, to include, the Criminal Investigator Training Program, the ATF Special Agent Basic Training Program, and the Homeland Security Investigations Special Agent Training Program. Prior to my employment with ATF, I was employed as a Special Agent with Homeland Security Investigations, in New York City. I have been involved in multiple investigations involving firearms violations, domestic and international narcotics violations, and violent crime.

6. Through my training and experience, I know the habits, methods, routines, practices, and procedures commonly employed by persons engaged in trafficking firearms and CDS. Traffickers use cellphones to coordinate with suppliers, customers, and co-conspirators. They frequently switch phones or use multiple phones to evade detection. I also know the techniques employed by traffickers to keep records of their trafficking activities, to conceal proceeds of their illegal conduct, and to evade law enforcement. For example, they use cellphones, addresses, and vehicles subscribed or registered to names other than their own in order to avoid detection by law enforcement.

7. Further, individuals involved with illegal activities tend to use their cellular devices to call or text accomplices after the crime has been committed. Additionally, an individual may communicate with another person to strategize and attempt to hide the belongings or merchandise

from the crime committed.

8. I also know, based on my training and experience, that individuals involved with drug trafficking and illegal firearm possession frequently use cellular telephones, communication devices, and other electronic media storage to further their illegal activities. Persons who have firearms tend to take photographs of the firearm and ammunition, which is stored on their electronic device. An individual may communicate with others in reference to the purchase of or the selling of firearms and CDS through their electronic devices. Individuals found with firearms and CDS often post pictures of evidence, fruits of the crime, and instrumentalities, on social media pages to show others with whom they are connected, and use cellular telephones to take these pictures.

9. Based upon my training and experience, I have learned the following:

- a. Firearms and drug trafficking are an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, drug trafficking is an illegal commercial activity that is characterized by regular, repeated criminal activity.
- b. Cellular telephones are an indispensable tool of the firearms and narcotics trafficking trade. Narcotic traffickers use cellular telephones, push-to-talk telephones, Short Message Service (SMS), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, in order to maintain contact with other conspirators and narcotic traffickers. In addition, narcotic traffickers will often change their cellphones following the arrest of a member of their Drug Trafficking Organization (DTO), or at random in order to frustrate law enforcement efforts.
- c. Drug traffickers keep and maintain records of their various activities. Such records are regularly concealed in a suspect's automobile, residence, office, and on his person, and that they take various forms. Documents commonly concealed by traffickers, include but are not limited to notes in code, deposit slips, wired money transactions, hidden bank accounts, photographs of co-conspirators, various forms of commercial paper, personal address books, notebooks, records, receipts, ledgers, travel receipts (rental receipts, airline tickets, bus tickets, and/or train tickets) both commercial and private, money orders and other papers relating to the ordering, transportation, sale

and distribution of controlled dangerous substances or other such documents which will contain identifying data on the co-conspirators. These items are kept in locations that are considered safe by the drug traffickers such as safety deposit boxes, residences, vehicles and on their person, where they have ready access to them. Drug traffickers often have several residences decreasing the likelihood of detection by law enforcement;

- d. Firearms and drug traffickers use cellular telephones, pagers and other electronic communications devices to facilitate illegal transactions. The electronically stored information on these devices is of evidentiary value in identifying other members of the firearms and drug trafficking conspiracy and establishing the relationship between these individuals, including photographs and other identifying information stored on these devices; they also use their cellphones to communicate on various social media platforms such as Facebook and Instagram; and,
- e. Drug traffickers use computers or other electronic storage media, including smart phones, to store the records documents, take and store photographs and videos of co-conspirators, and contraband or items listed in paragraphs (c) and (d).

10. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search the **SUBJECT TELEPHONES**, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. I have not, however, excluded any information known to me that would defeat a determination of probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents and intercepted conversations, as well as conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

III. PROBABLE CAUSE

A. BACKGROUND

11. At approximately 9:00 pm on November 6, 2020, Baltimore City Police Department Detectives in a marked vehicle were traveling southbound in the 500 block of

Millington Avenue. Detectives observed a black Honda stopped in the travel lane at the intersection of Christian Street and Millington Avenue. The two occupants appeared to be speaking with several individuals standing around the Honda. Detectives noticed that the Honda's rear windows appeared to be illegally tinted. The front windows were rolled down, and the detectives saw the front passenger holding an unsecured infant in the front seat. When the Honda driver—later identified as Antwon FRASIER—noticed the detectives' presence, he backed up and pulled next to the curb.

12. Detectives initiated a traffic stop, approached, and immediately smelled a strong odor of marijuana coming from the inside of the vehicle. Detectives asked FRASIER to step out of the vehicle and learned that he did not possess a driver's license. FRASIER then consented to a pat down. During the pat down, detectives recovered a Ruger LC9 pistol, 9mm, serial number #325-00865, loaded with eight live rounds of 9mm ammunition from FRASIER's waist. Detectives placed FRASIER under arrest, recovered the **SUBJECT TELEPHONES**, and issued traffic citations for the window tint, failing to secure the infant, and driving without a license.

13. The Ruger did not expel a projectile when it was test-fired by the BPD Firearms Lab because it did not contain a firing pin. Based on my training and experience, and having consulted with an ATF firearms expert, the firearm is nonetheless readily convertible to expel a projectile. Likewise, the frame and receiver of the Ruger is considered a firearm. Therefore, the firearm meets the definition a firearm under 18 U.S.C. § 921(a)(3). The firearm was not manufactured in Maryland and was recovered in Maryland; therefore, it affected interstate commerce.

14. Furthermore, the Ruger contained eight rounds of live ammunition as follows:

- a. Three Speer, jacketed round nose 9mm cartridges;

- b. Two Winchester jacketed round nose 9mm cartridges;
- c. Two PMC jacketed hollow point 9mm cartridges; and,
- d. One Winchester jacketed hollow point 9mm cartridge.

15. I have spoken to an ATF interstate nexus expert and learned that the ammunition was manufactured outside of Maryland and recovered in Maryland. Therefore, the ammunition also affected interstate commerce.

16. Prior to the events set forth in this affidavit, FRASIER was convicted of Possession with the Intent to Distribute Narcotics by the Circuit Court of Baltimore City and sentenced to three years in prison, with two years, 11 months, and 27 days suspended. Because the conviction resulted in a sentence of over one year, there is probable cause to believe that FRASIER was aware of his status at the time he possessed the firearm.

IV. BACKGROUND CONCERNING ELECTRONIC COMMUNICATIONS DEVICES

17. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of tools and instrumentalities of pending criminal activity. The **SUBJECT TELEPHONES** have both digital storage capacity and digital camera capabilities.

18. Individuals engaged in firearms and drug trafficking offenses often use cell phones to communicate with suppliers, to place orders with suppliers, to communicate with customers, to receive orders from customers, and to arrange meeting times and locations for the distribution of controlled substances. The individuals engaging in firearms and drug trafficking will often use a combination of voice calls and text messages to coordinate drug transactions. Individuals engaged in drug trafficking offenses also use digital storage devices to maintain telephone number “contact lists” of individuals who may have assisted in the planning of this and other criminal activity.

19. Firearms and narcotic traffickers often place nominal control and ownership of telephones in names other than their own to avoid detection of those telephones by government agencies. Even though telephones are in the names of other people, drug traffickers retain actual ownership, control, and use of the telephone, exercising dominion and control over them.

20. Criminals utilize different types of communication devices, and change the numbers to these communication devices frequently. This is done to avoid detection by law enforcement personnel. Also, as noted above, firearms and drug traffickers dedicate different communication devices for different aspects of the trafficking organization.

21. Cellular phones associated with firearms and drug traffickers include various types of evidence. Phones may contain relevant text messages or other electronic communications; they may contain electronic address books listing the phone numbers and other contact information associated with co-conspirators; and they may contain other types of information.

22. Criminals often take photos of themselves with firearms, large quantities of controlled substances, money, or high-end consumer items, like cars or watches. These “trophy” photos are often maintained on cellular telephones to be shared on social media, or as symbols of their success.

23. Finally, the mere fact of a cellular phone’s call number, electronic serial number or other identifying information may be of evidentiary value as it may confirm that a particular cell phone is the phone identified during a wiretap, pen register, or other electronic investigation.

V. FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

24. Based on my training and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This

information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT TELEPHONES** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

25. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT TELEPHONES** were used, the purpose of its use, who used it, and when.

26. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT TELEPHONES** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

27. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

28. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how

electronic devices were used, the purpose of their use, who used them, and when.

29. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

30. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. During this case and in numerous others involving complex DTOs, investigators have learned that the drug-trafficking organization relies heavily on electronic devices to facilitate drug trafficking. It is necessary to conduct a physical inspection of the electronic devices in order to obtain electronic communications and other information that might be stored on the seized phone and to determine whether any of the seized phone were the subject of wiretap, pen register or other investigation detailed herein. The phone may also contain data and communications that were not electronically intercepted due to encryption or for other reasons.

32. The device will be examined by persons qualified to perform the search / examination, with any and all necessary and proper assistance, any and all electronic computing or data processing devices and associated peripheral equipment such as computer units, keyboards, central processing units, external or internal drives and/or other receiving devices and peripheral equipment such as printers, modems, associated telephone sets, and any other controlling devices

and generate copies and photograph any evidence seized and any evidence therein. If needed, the processing may be conducted by a law enforcement entity or facility outside the state of Maryland.

33. Again, the **SUBJECT TELEPHONES** remain in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are detailed in Attachment A and the types of information expected to be recovered from the devices are listed in Attachment B.

VI. CONCLUSION

34. Accordingly, there is probable cause to believe that evidence will be found from an analysis of the recovered **SUBJECT TELEPHONES**. The **SUBJECT TELEPHONES** may contain the records of the most recent calls, which may include calls with persons involved in the offense(s). The **SUBJECT TELEPHONES** may contain copies of SMS or text or other electronic communications relating to activities associated with the offense(s). The **SUBJECT TELEPHONES** may also contain a variety of other electronic evidence, including electronic communications through various cellular or internet-based applications, photographs and other information.

35. Wherefore, in consideration of the facts presented, I respectfully request that this Court issue a search warrant for the **SUBJECT TELEPHONES**, and authorize the search of the items described in Attachment A, for the information set forth in Attachment B, where applicable, which constitute fruits, evidence and instrumentalities of the **SUBJECT OFFENSE**.

VII. REQUEST FOR NIGHT-TIME AUTHORIZATION

36. There is good cause for the Court to authorize the requested searches at any time of the day or night. The **SUBJECT TELEPHONES** are already in law enforcement custody, and it is reasonable to allow law enforcement to execute the requested searches at any hour of the day,

1:21-mj-461 TMD

even during the evening or night, if doing so is convenient for the investigators or examiners. Because the devices are already in law enforcement custody, there will be no prejudice to any other person from this request.

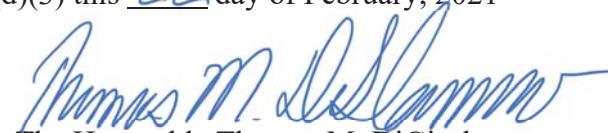
I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully submitted,

Joshua Futter Digital signature of Joshua Futter
Date: 2021.02.18 14:44:11 -05'00'

Special Agent Joshua Futter
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 22 day of February, 2021


The Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A
Device to be Searched

The following devices, currently in the custody of the ATF in the District of Maryland:

- a. a Black Apple iPhone, model 8 Plus, bearing IMEI No. 352978098922611
- b. a Black and silver Apple iPhone, model 6s, bearing IMEI No. 353338075591211

ATTACHMENT B
Items to be Seized

All records contained in the items described in Attachment A, which constitute evidence of the **SUBJECT OFFENSE**, including but not limited to those outlined below:

1. Contact logs that refer or relate to the user of any and all numbers on the Subject Electronic Devices.
2. Call logs reflecting date and time of received calls.
3. Any and all digital images and videos of persons associated with this investigation.
4. Text messages to and from the **SUBJECT TELEPHONES** that refer or relate to the crimes under investigation.
5. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.
6. Voicemails that refer or relate to the crimes under investigation.
7. Voice recordings that refer or relate to the crimes under investigation.
8. Any data reflecting the phone's location.
9. Contact lists.
10. Any and all records related to the location of the user(s) of the devices.
11. For the **SUBJECT TELEPHONES**:
 - a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the **SUBJECT TELEPHONES** of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;
 - f. evidence of the times the **SUBJECT TELEPHONES** were used;

- g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT TELEPHONES**;
- h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the **SUBJECT TELEPHONES**; and,
- i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
2. “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
3. “scanning” storage areas to discover and possibly recover recently deleted files;
4. “scanning” storage areas for deliberately hidden files; or
5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps

to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated, absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.